

On the Diophantine equation

$$X^{2N} + 2^{2\alpha}5^{2\beta}p^{2\gamma} = Z^5$$

Eva G. Goedhart and Helen G. Grundman

Abstract

We prove that for each odd prime p , positive integer α , and non-negative integers β and γ , the Diophantine equation $X^{2N} + 2^{2\alpha}5^{2\beta}p^{2\gamma} = Z^5$ has no solution with $X, Z, N \in \mathbb{Z}^+$, $N > 1$, and $\gcd(X, Z) = 1$.

1 Introduction

In 2001, Arif and Abu Muriefah [1] (and in 2002, independently, Le [13]) proved that there is no integer solution to the equation $x^2 + 2^{2m} = y^n$, with $m \geq 3$, $n \geq 3$, and $\gcd(x, y) = 1$. Since that time, there has been great interest in studying many variations of this equation. Of particular interest here are those in which the 2^{2m} is replaced by a power of a different prime or with the product of a small number of primes raised to powers. We consider an equation of the latter form, in which we also replace the variable exponent in the final term with the constant 5 and allow for any even exponent greater than 2 on the first term. Our equation is actually inspired by the work of Bennett [2] in which he considers the equation $x^{2n} + y^{2n} = z^5$, with $n > 1$. We do not require that the middle term be raised to the power $2n$, only that it be an even square with few prime factors.

Theorem 1. *Let p be an odd prime, α a positive integer, and β and γ non-negative integers. The equation*

$$X^{2N} + 2^{2\alpha}5^{2\beta}p^{2\gamma} = Z^5 \tag{1}$$

has no solution with $X, Z, N \in \mathbb{Z}^+$, $N > 1$, and $\gcd(X, Z) = 1$.

Note that the condition $N > 1$ is necessary for the theorem to hold, since, for example, $41^2 + 2^2 \cdot 19^2 = 5^5$.

A number of special cases of Theorem 1 are already known. For $N = 2$, Bruin [6, Theorem 1.1] proved that equation (1) has no positive integer solutions and for $N = 3$, Bennett and Chen [3, Theorem 1] proved likewise. The theorem is also known to be true for $\beta = \gamma = 0$ [1, 13], $\beta \neq 0$ and $\gamma = 0$ [15], $p = 3$ and $\beta = 0$ [14], $p = 11$ and $\beta = 0$ [7], $p = 13$ [12], $p = 17$ [11], $p = 19$ and $\beta = 0$ [16], $2^{2\alpha}5^{2\beta}p^{2\gamma} \leq 100$ (see, for example, [5]), and N divisible by a prime greater than 17 that is congruent to 1 modulo 4 [8].

We note further that, since equation (1) is of the form $X^{2N} + C^2 = Z^5$, a result of Darmon and Granville [10, Theorem 2] guarantees that, for any given value of N , there are at most finitely many integer solutions with $\gcd(X, Z) = 1$.

In the following section, we first present and prove a lemma important to the proof of Theorem 1. We then state a simplified version of a result due to Bennett and Skinner [4], specific to our needs. In Section 3, we prove Theorem 1, following the ideas and methods found in [2].

2 Preliminaries

We begin with two lemmas.

Lemma 2. *Let p , α , β , and γ be as in Theorem 1, with $p \neq 5$. Let u and $v \in \mathbb{Z}$ be coprime, with v even, such that*

$$2^\alpha 5^\beta p^\gamma = v(v^4 - 10u^2v^2 + 5u^4). \quad (2)$$

Then $v^4 - 10u^2v^2 + 5u^4 \neq 5$.

Proof. Suppose that $v^4 - 10u^2v^2 + 5u^4 = 5$. Then, by equation (2),

$$v = 2^\alpha 5^{\beta-1} p^\gamma$$

and $\beta \geq 2$. Combining the two equations, we find that $5(u^2 - v^2)^2 - 5 = 4v^4 = 2^{4\alpha+2} 5^{4\beta-4} p^{4\gamma}$, and so $(u^2 - v^2 + 1)(u^2 - v^2 - 1) = 2^{4\alpha+2} 5^{4\beta-5} p^{4\gamma}$. Since $\gcd(u^2 - v^2 + 1, u^2 - v^2 - 1) = 2$ and $u^2 - v^2 + 1 \equiv 2 \pmod{4}$,

$$u^2 - v^2 + 1 = 2 \cdot 5^k p^\ell \quad \text{and} \quad u^2 - v^2 - 1 = 2^{4\alpha+1} 5^{k'} p^{\ell'},$$

where $\{k, k'\} = \{0, 4\beta - 5\}$ and $\{\ell, \ell'\} = \{0, 4\gamma\}$. Subtracting, then dividing by 2, we obtain

$$5^k p^\ell - 2^{4\alpha} 5^{k'} p^{\ell'} = 1. \quad (3)$$

Now, $2^4 \equiv 1 \pmod{5}$ and, since $p \neq 5$, $p^4 \equiv 1 \pmod{5}$. Hence, equation (3) implies that $k = 0$. It follows that $\ell \neq 0$ and so we have $p^{4\gamma} - 2^{4\alpha} 5^{4\beta-5} = 1$ with $\gamma \neq 0$. If $p \neq 3$, then reducing modulo 3 yields a contradiction. Thus $p = 3$ and

$$3^{4\gamma} - 2^{4\alpha} 5^{4\beta-5} = 1. \quad (4)$$

But this provides a positive integer solution to the equation $X^2 + 2^a \cdot 5^b = Y^N$ with $\gcd(X, Y) = 1$, $4 \mid N$, $a > 0$, and $b \geq 3$, contradicting [15, Theorem 1.1].

Therefore, $v^4 - 10u^2v^2 + 5u^4 \neq 5$. \square

Following a “modular approach” to solving Diophantine equations, Bennett and Skinner [4] developed the main tools we use in proving Theorem 1. We give here a corollary of a particular case of one of their results, based on the presentation given in [9, Theorem 15.8.3]. As usual, for $a \in \mathbb{Q}$, let $v_p(a)$ denote the p -valuation of a .

Lemma 3 (Bennett-Skinner). *Let $x^7 + Cy^7 = z^2$ with $C, x, y, z \in \mathbb{Z}$, $xy \neq \pm 1$, x, Cy , and z nonzero and pairwise relatively prime, $z \equiv 1 \pmod{4}$, $v_2(Cy^7) \geq 6$, and for all primes q , $v_q(C) < 7$. Then there exists a newform of level*

$$N_7 = \begin{cases} 2\text{rad}(C), & \text{if } v_2(C) = 0, \\ \text{rad}(C)/2, & \text{if } v_2(C) = 6, \\ \text{rad}(C), & \text{otherwise.} \end{cases}$$

3 Proof of Theorem 1

Let p, α, β , and γ be as in Theorem 1 and suppose that $(N, X, Z) = (n, x, z)$ is a solution to equation (1) with $n, x, z \in \mathbb{Z}^+$, $n > 1$, and $\gcd(x, z) = 1$. Note that, since $\alpha \geq 1$, x and z are both odd.

We assume without loss of generality that $p \neq 5$ and that n is prime. As noted in the introduction, by [6], $n \neq 2$, and by [3], $n \neq 3$.

Suppose that $n = 5$. By equation (1),

$$x^{10} + 2^{2\alpha}5^{2\beta}p^{2\gamma} = z^5, \quad (5)$$

and so

$$2^{2\alpha}5^{2\beta}p^{2\gamma} = (z - x^2)(z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8). \quad (6)$$

Since x and z are odd, $z - x^2$ is even. Note that, since $x \geq 1$ and $\alpha \geq 1$, $x^{10} + 2^{2\alpha}5^{2\beta}p^{2\gamma} \geq 5$, which implies that $z > 1$, and, therefore, $z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8 \neq 1$ or 5 .

If $\beta = 0$, then $\gcd(z - x^2, z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8) = 1$ and so

$$z - x^2 = 2^{2\alpha} \text{ and } z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8 = p^{2\gamma}.$$

If $\beta \neq 0$, then, noting that $z - x^2 \equiv z^5 - x^{10} \equiv 0 \pmod{5}$, we have $5 \mid (z - x^2)$. So $z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8 \equiv 5 \pmod{25}$ and $\gcd(z - x^2, z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8) = 5$. Hence, from equation (6),

$$z - x^2 = 2^{2\alpha}5^{2\beta-1} \text{ and } z^4 + z^3x^2 + z^2x^4 + zx^6 + x^8 = 5p^{2\gamma}.$$

Thus, in either case, we have $z = x^2 + 2^{2\alpha}5^j$, with $j \geq 0$. So equation (5) becomes $2^{2\alpha}5^{2\beta}p^{2\gamma} = (x^2 + 2^{2\alpha}5^j)^5 - x^{10}$. Expanding and removing a factor of $2^{2\alpha}$, we have

$$5^{2\beta}p^{2\gamma} = 5^{j+1}x^8 + 2^{2\alpha+1}5^{2j+1}x^6 + 2^{4\alpha+1}5^{3j+1}x^4 + 2^{6\alpha}5^{4j+1}x^2 + 2^{8\alpha}5^{5j}. \quad (7)$$

If $\beta = 0$, then $j = 0$ and reducing equation (7) modulo 8 yields $1 \equiv 5 \pmod{8}$, a contradiction. If $\beta \neq 0$, then $j = 2\beta - 1$ and reducing equation (7) modulo 3 yields $p^{2\gamma} \equiv 2 \pmod{3}$, another contradiction. Hence, $n \neq 5$.

So $n \geq 7$.

Writing equation (1) in the form $(x^n)^2 + (2^\alpha 5^\beta p^m)^2 = z^5$, a classical argument (see, for example, [9, Section 14.2]) yields nonzero coprime integers, u and v , of opposite parity, such that

$$x^n = u(u^4 - 10u^2v^2 + 5v^4) \quad (8)$$

and

$$2^\alpha 5^\beta p^\gamma = v(v^4 - 10u^2v^2 + 5u^4). \quad (9)$$

Since x is odd, equation (8) implies that u is odd. Since u and v are of opposite parity, v is even.

Further, since $\gcd(u, v) = 1$,

$$\gcd(v, v^4 - 10u^2v^2 + 5u^4) = \gcd(v, 5).$$

If $5 \mid v$, then $5 \nmid u$ and so $v^4 - 10u^2v^2 + 5u^4 \equiv 5 \pmod{25}$. Thus, since $\gcd(v, v^4 - 10u^2v^2 + 5u^4) = 5$, by equation (9), $v^4 - 10u^2v^2 + 5u^4 = 5$ or $\pm 5p^\gamma$. By Lemma 2, the first is impossible. Therefore, we have

$$v = \pm 2^\alpha 5^{\beta-1} \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm 5p^\gamma, \quad (10)$$

with $\gamma \neq 0$.

If $5 \nmid v$, then, by equation (9), $\beta = 0$. Since $\gcd(v, v^4 - 10u^2v^2 + 5u^4) = 1$, $v^4 - 10u^2v^2 + 5u^4 = \pm 1$ or $\pm p^\gamma$. But $v^4 - 10u^2v^2 + 5u^4 \equiv 5 \pmod{8}$, since v is even. Hence, in this case,

$$v = \pm 2^\alpha \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm p^\gamma. \quad (11)$$

Combining equations (10) and (11), we have

$$v = \pm 2^\alpha 5^k \quad \text{and} \quad v^4 - 10u^2v^2 + 5u^4 = \pm 5^{\beta-k} p^\gamma, \quad (12)$$

where $k = \beta - 1$ if $5 \mid v$, and $k = 0$ otherwise.

Now, if $5 \mid u$, then $5 \nmid v$ and we have $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = 5$. Since $u^4 - 10u^2v^2 + 5v^4 \equiv 5 \pmod{25}$ and n is odd, by equation (8), there exist nonzero coprime integers $A_1, B_1 \in \mathbb{Z}$ such that

$$u = 5^{n-1} A_1^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = 5B_1^n. \quad (13)$$

Thus, $5B_1^n + 20v^4 = (u^2 - 5v^2)^2$. Recalling that $5 \nmid v$, we can combine this with equation (11), letting $w_1 = (u^2 - 5v^2)/5 \in \mathbb{Z}$, to obtain

$$B_1^n + 2^{4\alpha+2} = 5w_1^2. \quad (14)$$

Reducing the second part of (13) modulo 8, we find that $1 \equiv 5B_1^n \pmod{8}$, and hence B_1 is odd and not equal to ± 1 . By [4, Theorem 1.2], there is no integer solution to the equation $X^n + 2^{4\alpha+2}Y^n = 5Z^2$, satisfying these conditions. Thus, we have a contradiction.

On the other hand, if $5 \nmid u$, then $\gcd(u, u^4 - 10u^2v^2 + 5v^4) = 1$. This together with equation (8) and the fact that n is odd implies that there exist nonzero coprime integers $A_2, B_2 \in \mathbb{Z}$ such that

$$u = A_2^n \quad \text{and} \quad u^4 - 10u^2v^2 + 5v^4 = B_2^n. \quad (15)$$

Thus, $B_2^n + 20v^4 = (u^2 - 5v^2)^2$. Combining this with equation (12) and letting $w_2 = u^2 - 5v^2$ yields

$$B_2^n + 2^{4\alpha+2}5^{4k+1} = w_2^2. \quad (16)$$

By equation (15), since u is not divisible by 2 or 5, neither is B_2 . So $\gcd(B_2, w_2) = 1$. By [4, Theorem 1.5], there is no integer solution to the equation $X^n + 2^{4\alpha+2}5^{4k+1}Y^n = Z^2$, satisfying these conditions, with prime $n \geq 11$. Hence, we have a contradiction unless $n = 7$.

For the case $n = 7$ (still assuming that $5 \nmid u$), we first note that $4\alpha + 2 \geq 6$, $w_2 \equiv 1 \pmod{4}$, and, since $\gcd(u, v) = 1$, $3 \nmid w_2$. Evaluating equation (16) modulo 3, recalling that $n = 7$, yields $B_2^7 + 2 \equiv 1 \pmod{3}$, implying that $B_2 \equiv 2 \pmod{3}$. On the other hand, evaluating equation (16) modulo 8 yields $B_2 \equiv B_2^7 \equiv w_2^2 \equiv 1 \pmod{8}$. Thus $B_2 \neq \pm 1$.

Rewriting equation (16) in the form

$$B_2^7 + 2^{r_1}5^{r_2}(2^{s_1}5^{s_2})^7 = w_2^2,$$

with $r_i, s_i \in \mathbb{Z}$ such that $0 \leq r_i < 7$, for $i \in \{1, 2\}$, we can apply Lemma 3 (with $C = 2^{r_1}5^{r_2}$). Hence, there exists a newform of level N_7 , where $N_7 \in \{1, 2, 5, 10\}$. But, as is well-known (see, for example, [9, Corollary 15.1.2]), there are no newforms of any of these levels. Therefore $n \neq 7$, yielding another contradiction.

Hence the initial supposition is false, and the theorem is proved.

References

- [1] S. A. Arif and F. S. Abu Muriefah, “On the Diophantine equation $x^2 + 2^k = y^n$, II”, *Arab J. Math. Sci.*, **7** (2001), no. 1, 67–71.
- [2] M. A. Bennett, “The equation $x^{2n} + y^{2n} = z^{5n}$ ”, *J. Théor. Nombres Bordeaux* **18** (2006), no. 2, 315–321.
- [3] M. A. Bennett and I. Chen “Multi-Frey \mathbb{Q} -curves and the Diophantine equation $a^2 + b^6 = c^n$ ”, *Algebra Number Theory* **6** (2012), no. 4, 707–730.
- [4] M. A. Bennett and C. M. Skinner, “Ternary Diophantine equations via Galois representations and modular forms”, *Canad. J. Math.* **56** (2004), no. 1, 23–54.
- [5] Y. Bugeaud, M. Mignotte, and S. Siksek, “Classical and modular approaches to exponential Diophantine equations II. The Lebesgue-Nagell equation”, *Compositio Math.*, **142** (2006), 31–62.
- [6] N. Bruin, “Chabauty methods using elliptic curves”, *J. reine angew. Math.* **562** (2003), 27–49.
- [7] I. N. Cangül, M. Demirci, F. Luca, Á. Pintér, and G. Soydan, “On the Diophantine equation $x^2 + 2^a \cdot 11^b = y^n$ ”, *Fibonacci Q.*, **48** (2010), no. 1, 39–46.

- [8] I. Chen, “On the equation $a^2 + b^{2p} = c^5$ ”, *Acta Arith.* **143** (2010), no. 4, 345–375.
- [9] H. Cohen, *Number Theory, Vol. II: Analytic and Modern Tools, GTM*, **240**, Springer, New York, 2007.
- [10] H. Darmon and A. Granville, “On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$ ”, *Bull. London Math. Soc.* **27** (1995), no. 6, 513–544.
- [11] H. Godinho, D. Marques, and A. Togbé, “On the Diophantine equation $x^2 + 2^\alpha 5^\beta 17^\gamma = y^n$ ”, *Commun. Math.*, **20** (2012), no. 2, 81–88.
- [12] E. Goins, F. Luca, and A. Togbé, “On the Diophantine equation $x^2 + 2^\alpha 5^\beta 13^\gamma = y^n$ ”, *Lecture Notes in Computer Science*, **5011**, A. J. van der Poorten and A. Stein (eds.), Springer, Berlin, 2008.
- [13] M. H. Le, “On Cohn’s conjecture concerning the Diophantine equation $x^2 + 2^m = y^n$ ”, *Arch. Math. (Basel)*, **78** (2002), no. 1, 26–35.
- [14] F. Luca, “On the equation $x^2 + 2^a \cdot 3^b = y^n$ ”, *Int. J. Math. Math. Sci.*, **29** (2002), no. 4, 239–244.
- [15] F. Luca and A. Togbé, “On the Diophantine equation $x^2 + 2^a \cdot 5^b = y^n$ ”, *Int. J. Number Th.*, **4** (2008), no. 6, 973–979.
- [16] G. Soydan, M. Ulas, H. L. Zhu, “On the Diophantine equation $x^2 + 2^a \cdot 19^b = y^n$ ”, *Indian Journal of Pure and Applied Mathematics*, **43** (2012), 251–261.

Department of Mathematics
 Bryn Mawr College
 Bryn Mawr, PA 19010
 egoedhart@brynmawr.edu
 grundman@brynmawr.edu